IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

Accessing a Server Using a User Authentication Indicator

Inventor(s):
John Hal Howard
Jeffrey C. Kunins
Darren L. Anderson
Ryan W. Battle
Max E. Metral

ATTORNEY'S DOCKET NO. MS1-367USC1

RELATED APPLICATIONS

This application is a continuation of U.S. Application Serial No. 09/350,018 filed July 8, 1999 and entitled "Controlling Access To A Network Server Using An Authentication Ticket", incorporated by reference herein for all that it discloses and teaches.

TECHNICAL FIELD

This invention relates to network access systems. More particularly, the invention relates to the control of access to a network by a user through an authentication server that generates an authentication ticket indicating whether the user has been authenticated.

BACKGROUND OF THE INVENTION

The recent growth in popularity of the Internet has significantly increased the number of Internet users and the number of Internet sites (also referred to as "web sites"). Web sites may provide various types of information to users, offer products or services for sale, and provide games and other forms of entertainment. Many web sites require users to "register" by providing information about themselves before the web server grants access to the site. This registration information may include the user's name, account number, address, telephone number, email address, computer platform, age, gender, or hobbies. The registration information collected by the web site may be necessary to complete transactions (such as commercial or financial transactions). Additionally, information can be collected which allows the web site operator to learn about the visitors to the site to better target its future marketing activities or adjust the

information provided on the web site. The collected information may also be used to allow the web site to contact the user directly (e.g., via email) in the future to announce, for example, special promotions, new products, or new features of the web site.

When registering with a web site for the first time, the web site typically requests that the user select a login ID and an associated password. The login ID allows the web site to identify the user and retrieve the user's information during subsequent user visits to the web site. Generally, the login ID must be unique to the web site such that no two users have the same login ID. The password associated with the login ID allows the web site to authenticate the user during subsequent visits to the web site. The password also prevents others (who do not know the password) from accessing the web site using the user's login ID. This password protection is particularly important if the web site stores private or confidential information about the user, such as financial information or medial records.

If a user visits several different web sites, each web site may require entry of similar registration information about the user, such as the user's name, mailing address, and email address. This repeated entry of identical data is tedious when visiting multiple web sites in a short period of time. Many web sites require the user to register before accessing any information provided on the web site. Thus, the user must enter the requested registration information before they can determine whether the site contains any information of interest.

After registering with multiple web sites, the user must remember the specific login ID and password used with each web site or other Internet service. Without the correct login ID and password, the user must re-enter the registration

information. A particular user is likely to have different login IDs and associated passwords on different web sites. For example, a user named Bob Smith may select "smith" as his login ID for a particular site. If the site already has a user with a login ID of "smith" or requires a login ID of at least six characters, then the user must select a different login ID. After registering at numerous web sites, Bob Smith may have a collection of different login IDs, such as: smith, smith1, bsmith, smithb, bobsmith, bob_smith, and smithbob. Further, different passwords may be associated with different login IDs due to differing password requirements of the different web sites (e.g., password length requirements or a requirement that each password include at least one numeric character). Thus, Bob Smith must maintain a list of web sites, login IDs, and associated passwords for all sites that he visits regularly.

SUMMARY OF THE INVENTION

A mechanism for seeking access of a client to a first server is described. The mechanism involves determining that a client seeking access to the first server is not authenticated by an authentication server. The mechanism further involves communicating a request for login information to be returned to the second server from the client. Login information is received at the authentication server from the client. The client is authenticated by comparing the login information with authentication information maintained by the authentication server. When the login information matches the authentication information, a user authentication indicator (which in one version is an authentication ticket) is generated at the authentication server and the user sends the authentication indicator to the first

server.

An implementation of the invention receives a request from a network server to authenticate a user who is seeking access to the network server. The process determines whether the user was already authenticated by the authentication server. If the user was already authenticated, then the network server is notified that the user is authenticated through the use of a user authentication indicator. If the user was not already authenticated by the authentication server, then login information is retrieved from the user and compared to authentication information maintained by the authentication server. The network server is notified (through the use of the user authentication indicator) that the user is authenticated if the retrieved login information matches the authentication information.

Other aspects of the invention provide for the user authentication indicator that does not contain any reference to the user's login information.

In accordance with another aspect of the invention, the user authentication indicator includes a first time stamp indicating the last time the user's login information was refreshed, and a second time stamp indicating the last time the user physically entered their login information.

In one embodiment of the invention, the network server is a web server coupled to the Internet.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates an exemplary network environment in which the present invention is utilized.

Fig. 2 is a block diagram showing pertinent components of a computer in accordance with the invention.

Figs. 3 and 4 illustrate the interaction between the client computer system, a particular affiliate server and the authentication server when a user of the client computer system seeks access to the affiliate server.

Figs. 5 and 6 illustrate the interaction between the client computer system, a particular affiliate server and the authentication server in a different situation.

DETAILED DESCRIPTION

Fig. 1 illustrates an exemplary network environment in which the present invention is utilized. A client computer system 100 is coupled to a network 102. In this example, network 102 is the Internet (or the World-Wide Web). However, the teachings of the present invention can be applied to any data communication network. Multiple affiliate servers 104, 106, and 108 are coupled to network 102, thereby allowing client computer system 100 to access web servers 104, 106, and 108 via the network. Affiliate servers 104, 106, and 108 are also referred to as "web servers" and "network servers". An authentication server 110 is also coupled to network 102, allowing communication between the authentication server and client computer system 100 and web servers 104, 106, and 108. Although referred to as an "authentication server", authentication server 110 is also a web server capable of interacting with web browsers and other web servers. In this example, data is communicated between the authentication server, client computer system, and web servers using the hypertext transfer protocol (http), a protocol commonly used on the Internet to exchange information.

An authentication database 112 is coupled to authentication server 110. The authentication database 112 contains information necessary to authenticate users and also identifies which elements of the user profile information should be provided to a particular affiliate server when the user accesses the affiliate server. Although the authentication database 112 is shown separately from the authentication server 110, in other embodiments of the invention, the authentication database is contained within the authentication server.

The authentication process, as described below, authenticates a user of client computer 100 seeking access to an affiliate server 104, 106, or 108. The authentication server 110 authenticates the user of client computer 100 by requesting authenticating information, such as the user's login ID and password. If the user is successfully authenticated, then authentication server 110 generates an authentication ticket and communicates the ticket to the appropriate affiliate server. The authentication ticket indicates that the user is authenticated. Additional details regarding the authentication ticket are provided below.

As part of the user authentication process, the authentication server 110 may provide certain user profile information to the affiliate server, such as the user's email address, user preferences, and the type of Internet browser installed on client computer 100. This user profile information is associated with the user's login ID so that each time the user logs into an affiliate server, the associated user profile information is available to provide to the affiliate server. This user profile allows the user to enter the information once and use that information during subsequent logins to new affiliate servers.

The term "affiliate server" is defined herein as a web server that has "registered" or otherwise established a relationship or affiliation with the

authentication server 110. Each affiliate server 104, 106, and 108 includes a code sequence (not shown) that allows the affiliate server to communicate with the authentication server 110 when a user (who is also registered with the authentication server) requests access to the affiliate server. Additional details regarding the authentication process and the interaction between the client computer, the affiliate servers, and the authentication server are provided below.

Fig. 2 shows a general example of a computer 130 that can be used with the present invention. A computer such as that shown in Fig. 2 can be used for client computer system 100, authentication server 110, or any of the affiliate servers 104, 106 or 108.

Computer 130 includes one or more processors or processing units 132, a system memory 134, and a bus 136 that couples various system components including the system memory 134 to processors 132. The bus 136 represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. The system memory 134 includes read only memory (ROM) 138 and random access memory (RAM) 140. A basic input/output system (BIOS) 142, containing the basic routines that help to transfer information between elements within computer 130, such as during start-up, is stored in ROM 138.

Computer 130 further includes a hard disk drive 144 for reading from and writing to a hard disk (not shown), a magnetic disk drive 146 for reading from and writing to a removable magnetic disk 148, and an optical disk drive 150 for reading from or writing to a removable optical disk 152 such as a CD ROM or other optical media. The hard disk drive 144, magnetic disk drive 146, and optical

disk drive 150 are connected to the bus 136 by an SCSI interface 154 or some other appropriate interface. The drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data for computer 130. Although the exemplary environment described herein employs a hard disk, a removable magnetic disk 148 and a removable optical disk 152, it should be appreciated by those skilled in the art that other types of computer-readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, random access memories (RAMs), read only memories (ROMs), and the like, may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk 144, magnetic disk 148, optical disk 152, ROM 138, or RAM 140, including an operating system 158, one or more application programs 160, other program modules 162, and program data 164. A user may enter commands and information into computer 130 through input devices such as a keyboard 166 and a pointing device 168. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to the processing unit 132 through an interface 170 that is coupled to the bus 136. A monitor 172 or other type of display device is also connected to the bus 136 via an interface, such as a video adapter 174. In addition to the monitor, personal computers typically include other peripheral output devices (not shown) such as speakers and printers.

Computer 130 commonly operates in a networked environment using logical connections to one or more remote computers, such as a remote computer

176. The remote computer 176 may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to computer 130, although only a memory storage device 178 has been illustrated in Fig. 2. The logical connections depicted in Fig. 2 include a local area network (LAN) 180 and a wide area network (WAN) 182. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets, and the Internet.

When used in a LAN networking environment, computer 130 is connected to the local network 180 through a network interface or adapter 184. When used in a WAN networking environment, computer 130 typically includes a modem 186 or other means for establishing communications over the wide area network 182, such as the Internet. The modem 186, which may be internal or external, is connected to the bus 136 via a serial port interface 156. In a networked environment, program modules depicted relative to the personal computer 130, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

Generally, the data processors of computer 130 are programmed by means of instructions stored at different times in the various computer-readable storage media of the computer. Programs and operating systems are typically distributed, for example, on floppy disks or CD-ROMs. From there, they are installed or loaded into the secondary memory of a computer. At execution, they are loaded at least partially into the computer's primary electronic memory. The invention described herein includes these and other various types of computer-readable

storage media when such media contain instructions or programs for implementing the steps described below in conjunction with a microprocessor or other data processor. The invention also includes the computer itself when programmed according to the methods and techniques described below.

For purposes of illustration, programs and other executable program components such as the operating system are illustrated herein as discrete blocks, although it is recognized that such programs and components reside at various times in different storage components of the computer, and are executed by the data processor(s) of the computer.

Prior to executing the authentication process described below, both the user of client computer system 100 and the operator of affiliate server 104 "register" with the authentication server 110. This registration is a one-time process which provides necessary information to the authentication server. The user of client computer system 100 registers by providing the user's name, mailing address, email address, and various other information about the user or the client computer system. As part of the user registration process, the user is assigned (or selects) a login ID, which is a common login ID used to access any affiliate server. The login ID may also be referred to herein as a "user name" or "login name". Additionally, the user selects a password associated with the login ID which is used for authentication purposes. After registering and logging into the authentication server, the user can visit any affiliate server (i.e., affiliate servers that are also registered with the same authentication server) without requiring any additional authentication and without re-entering user information that is already contained in the associated user profile.

The operator of affiliate server 104 registers with the authentication server 110 by providing information about the affiliate server (e.g., server name and internet address). Additionally, the affiliate server provides information regarding its authentication requirements. The authentication requirements can be specified as the maximum time allowed since the last login and entry of authentication information by the user as well as the maximum time allowed since the last "refresh" of the authentication information by the user. Refreshing the authentication information refers to the process of having the user re-enter the password to be certain that the appropriate user is still operating the client computer system. This periodic refreshing of authentication information is useful if the user leaves their computer system without logging out of the authentication server, thereby allowing another individual to access affiliate servers using the login ID of the previous user. If a user requests access to the affiliate server after the maximum time allowed, then the user is re-authenticated (i.e., refreshed) by the authentication server by issuing a new authentication ticket. Thus, although there is a central authentication server, each individual affiliate server can establish its own authentication requirements which are enforced by the authentication server. After registering with the authentication server, the affiliate server can use the authentication server to authenticate any user that has also registered with the authentication server.

Figs. 3 and 4 illustrate the interaction between the client computer system 100, the affiliate server 104, and the authentication server 110 when a user of the client computer system seeks access to the affiliate server. The example illustrated with respect to Figs. 3 and 4 describes the situation in which the user of the client computer system 100 has not yet logged into the affiliate server 104 and has not

yet been authenticated by the authentication server 110. The lines in Fig. 3 labeled "A" through "H" represent the flow of information or activities during the authentication process. The arrows on the lines indicate the direction of the process flow. The label "A" represents the beginning of the process and the label "H" represents the end of the process. The corresponding steps in Fig. 4 are indicated with the label in parenthesis.

Fig. 4 is a flow diagram illustrating the authentication process when a user of the client computer system 100 seeks access to the affiliate server 104. The process begins when the user of the client computer system accesses a web page on the affiliate server (step 200). The client computer system includes a web browser, such as the "Internet Explorer" web browser manufactured and distributed by Microsoft Corporation of Redmond, Washington, for accessing various web sites. The affiliate server determines whether the user seeking access to the server is already logged into the affiliate server (e.g., authenticated) at step 202. In this example, the user is not logged into the affiliate server, so the user must be authenticated before the affiliate server will allow access. To authenticate the user, the affiliate server redirects the user's browser to the authentication server.

In this example, the user has not yet logged into the authentication server. Thus, the authentication server generates a sign-in web page and communicates the web page to the client computer system for display on the user's browser (step 204). The sign-in web page requests the user's login ID and password, which were established when the user registered with the authentication server. The user fills-in the requested information on the sign-in web page and clicks a "sign-in"

button on the web page to send the information entered to the authentication server (step 206).

Upon receiving the information from the user of the client computer system, the authentication server compares the entered information with the information stored in the authentication database (step 208). If the user-entered information is not correct (i.e., does not match the information stored in the authentication database) then the authentication server generates and communicates a web page to the user indicating the login ID and password combination were not valid (step 210). The web page may give the user an opportunity to re-enter the login ID and password by returning to step 204. Confidential information (such as the login ID and password) is communicated using a secure protocol such as SSL (secure sockets layer). Various other secure protocols or encryption mechanisms can be used to communicate confidential information between the authentication server and the client computer system.

If the user-entered information is correct (i.e., matches the information stored in the authentication database) then the authentication server copies the appropriate cookies to the client computer system and redirects the user's browser to the affiliate server (step 212). A "cookie" is a piece of data provided to a web browser by a web server. The data (i.e., cookie) is sent back to the web server by the web browser during subsequent accesses to the web server. With respect to step 212, one cookie contains information regarding the date and time that the user was authenticated by the authentication server. Another cookie contains information regarding the user profile. The authentication server also updates (or creates) a cookie that contains a list of all sites (or web servers) visited by the user since the last logout from the authentication server. The cookie is updated by

adding the current affiliate server to the list of sites visited. This list of sites visited is used to remove cookies from the client computer system when the user logs out of the authentication server. For example, when the user logs out, the authentication server sends a message to each web server on the list of sites visited. Each message is a request for the web server to delete any cookies it placed on the client computer system (e.g., through a browser running on the client computer system).

Cookies written to the client computer system by the authentication server cannot be read by any affiliate server. Similarly, cookies written to the client computer system by a particular affiliate server cannot be read by any other affiliate server. The cookies written by an affiliate server are encrypted using a key that is unique to the affiliate server, thereby preventing other affiliate servers from reading the data stored in the cookies.

Step 212 also includes generating an authentication ticket and transmitting the ticket to the affiliate server. The authentication ticket is generated by the authentication server and indicates whether a particular user has been authenticated by the authentication server. To protect the user's password and other login information, the affiliate server receives the authentication ticket instead of the user's password and other login information. The authentication ticket indicates that the user is authenticated and how much time has elapsed since the user was last authenticated.

The authentication server also communicates the user profile information to the affiliate server (step 214) through the client computer system. In a particular embodiment of the invention, the user of the client computer system can specify during the registration process what types of profile information should be

provided to various types of web servers. For example, a user may specify that all commerce-related web servers should receive the user's mailing address, but restrict the mailing address from all other types of web sites.

After receiving the authentication ticket and the user's profile information, the affiliate server generates a personalized web page for the user and communicates the web page to the user's browser (step 216). Additionally, the affiliate server copies one or more cookies to the client computer system which include information indicating that the user of the client computer system has been authenticated and indicating the period of time during which the authentication is valid. Each time the user enters a new web page request on the same affiliate server, the data in the cookie is copied to the affiliate server along with the page request. Thus, the affiliate server will not repeatedly check the authentication of a user during each subsequent page request. However, if a particular period of time has passed (referred to as a timeout period) since the last authentication process by the authentication server, then the affiliate server may request a re-authorization of the user.

The authentication ticket discussed above contains two time stamps. The first time stamp indicates the last time that the user's login ID and password were physically typed by the user. The second time stamp indicates the last time that the user's login information was refreshed by the authentication server. This "refresh" of the user's login information can be performed "silently" or by manual entry of the login information (i.e., login ID and password) by the user. The refreshing of the user's login information is performed by the authentication server. Once completed, a new authentication ticket is issued to the affiliate server indicating the new time stamp values. If the refresh operation fails (i.e., the user

does not supply the correct login information), then the user is logged out of the authentication server and all affiliate servers.

Each affiliate server can specify the minimum time requirements for each time stamp in the authentication ticket. If either time stamp exceeds the minimum time requirement for the affiliate server, then the authentication server is contacted to re-authenticate (or refresh) the user login information and update the time stamps accordingly. Each authentication ticket is encrypted using the affiliate server's shared encryption key, thereby preventing other affiliate servers from viewing the authentication ticket.

If the user of the client computer system is new to the affiliate server, the affiliate server may request additional user information that is not already contained in the user profile. The additional information may include information unique to that site (e.g., account number) or information about the user's preferences and how the user intends to use the web site. Thus, although the user generates a user profile that is stored on the authentication server, the user may be required, during an initial visit to a web site, to provide additional information for the benefit of the associated web server. This additional information is then stored by the affiliate server such that the user will not be required to re-enter the data during subsequent visits to the same web site.

Although affiliate server 104 and authentication server 110 are both coupled to network 102 (see Fig. 1), no direct connections are shown in Fig. 3. In this embodiment of the invention, the affiliate server 104 and the authentication server 110 do not communicate directly with one another. Instead, communications between the affiliate server and the authentication server pass through the client computer system. However, in an alternate embodiment of the

invention, affiliate server 104 communicates directly with authentication server 110, using network 102 or another data communication medium. Thus, rather than communicating through client computer system 100, the communications flow directly between the authentication server and the affiliate server. Although the authentication server and the affiliate server communicate directly, the user's authentication information (e.g., password) is not exposed to the affiliate server.

After a user has logged into the authentication server, it is not necessary to re-enter the login ID, password, or other user information when accessing other affiliated web servers. The subsequent affiliate web servers accessed will determine from the authentication server that the user is already authenticated.

Figs. 5 and 6 illustrate the interaction between the client computer system, a particular affiliate server and the authentication server in a different situation. The example illustrated with respect to Figs. 5 and 6 describes the situation in which the client computer system 100 has already been authenticated by the authentication server 110 (e.g., when logging into a different affiliate server), but the client computer system is not yet logged into the affiliate server 104.

In this example, the user of the client computer system 100 accesses a web page on the affiliate server 104 (step 230). The affiliate server determines that the user is not authenticated (with respect to the affiliate server) and redirects the user's browser to the authentication server (step 232). Next, the authentication server retrieves the affiliate information entered during registration of the affiliate to determine whether the most recent authentication of the user is within the affiliate's timeout period (step 234). If the most recent authentication is not within the timeout period (i.e., not acceptable), then the authentication server retrieves

and authenticates the user's login ID and password (step 238) using, for example, the procedures discussed above with respect to Fig. 4.

If the most recent authentication is acceptable, then the authentication server copies the appropriate cookies to the client computer system and redirects the user's browser back to the affiliate server (step 240). Additionally, the authentication server generates an authentication ticket, which is communicated to the affiliate server. As discussed above, the authentication ticket indicates to the affiliate server that the user is authenticated. Furthermore, the authentication ticket includes two timestamps indicating the elapsed time since the last user authentication.

The authentication server also copies certain elements of the user's profile information to the affiliate server (step 242). The affiliate server then generates a personalized web page and communicates the web page to the user's browser (step 244). The affiliate server also copies a cookie to the client computer system containing information indicating that the user of the client computer system has been authenticated and indicating the period of time during which the authentication is valid. Each time the user enters a new web page request on the same affiliate server, the data in the cookie is copied to the affiliate server along with the page request. Thus, the affiliate server will not repeatedly check the authentication of a user during each subsequent page request.

In an embodiment of the invention, a particular affiliate server may utilize only a portion of the services available from the authentication server. For example, the affiliate server may perform its own authentication of the user, but requests the user profile information from the authentication server. In another example, the affiliate server may rely on the authentication server to authenticate

the user, but the affiliate server ignores the user profile information and, instead, collects information from the user itself.

In one embodiment of the invention, the same login ID is used to identify a particular user on all affiliate servers. However, this configuration presents a situation in which affiliate servers could exchange information collected about the user with other affiliate servers, relying on the common login ID. To avoid this situation, a second embodiment of the invention uses a different login ID for each of the affiliate servers. This use of different login IDs is transparent to the user, who only knows of the login ID used to log into the authentication server. The authorization server maintains a list or cross-reference table that correlates the user's login ID on the different affiliate servers. In this embodiment, the affiliate servers do not know the login ID used on other affiliate servers for the same user and, therefore, cannot exchange information about the user with other affiliate servers.

A particular embodiment of the invention has been described and illustrated herein with reference to multiple web servers and an authentication server coupled to a common data communication network. However, the teachings of the present invention can be applied to any type of web server or other computing device that accesses a centralized authentication system to authenticate a user and retrieve associated user profile information. Furthermore, the present invention can be utilized without requiring a data communication network. Instead, one or more temporary or permanent data communication links are established between an authentication server and an affiliate server for exchanging data.

Thus, a system has been described that allows a web server to authenticate a user seeking access to the web server. The authentication is performed by an

authentication server without exposing the user's authentication information (e.g., password) to the web server. The web server receives an authentication ticket from the authentication server indicating whether the authentication was successful and further indicating the time since the last user authentication. The authentication server may also provide user profile information to the web server if the user is authenticated. Thus, the authentication server provides a centralized device for authenticating users without exposing the user's confidential login information to an affiliate server. This single user profile may be provided to multiple affiliate servers without requiring repeated entry of information by the user (i.e., entering user information at each new web site visited). Once the user has been authenticated by the authentication server, the user can visit multiple web sites that are affiliated with the authentication server without re-entering the authentication information for each web site.

Although the invention has been described in language specific to structural features and/or methodological steps, it is to be understood that the invention defined in the appended claims is not necessarily limited to the specific features or steps described. Rather, the specific features and steps are disclosed as preferred forms of implementing the claimed invention.